SN 10/588,608

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003186753 A**

(43) Date of publication of application: **04.07.03**

(51) Int. Cl **G06F 12/14**
G06F 1/00
G06F 1/24

(21) Application number: **2001388639**

(22) Date of filing: **21.12.01**

(71) Applicant: **CANON ELECTRONICS INC**

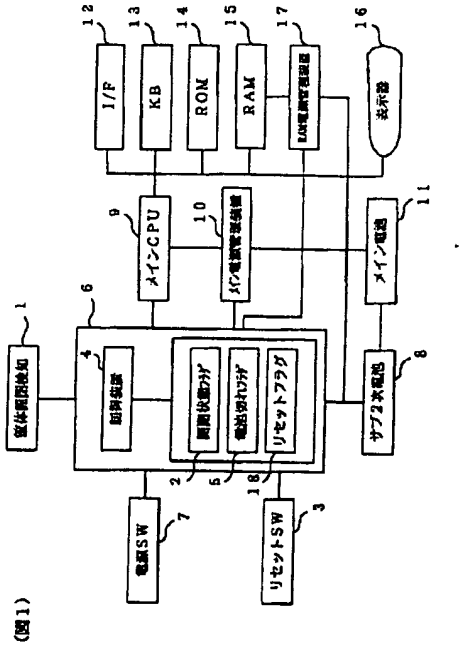
(72) Inventor: **AMARI TAKASHI**

(54) **ELECTRONIC DEVICE, CONTROL METHOD OF ELECTRONIC DEVICE AND CONTROL PROGRAM OF ELECTRONIC DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To attain both of tamper resistance and maintenance ability of an electronic device.

SOLUTION: When a chassis open/close state flag 2 indicates openness of the chassis in the past, an operation of an apparatus via a predetermined shell is approved only when reset booting is instructed by a reset switch 3, while normal booting of the apparatus is prohibited when reset boosting is not instructed by the reset switch 3. In the operation of the apparatus via the shell, the chassis open/close state flag 2 is reset to a state indicating cloure by initializing an inside data memory device. Protection of data is attained by breaking or prohibiting duplication of contents in a memory device (RAM 15) when the chassis open/close state flag 2 indicates openness of the chassis in the past.



(図1)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－186753
（P2003－186753A）
(43)公開日　平成15年７月４日(2003.7.4)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
G06F 12/14	320	G06F 12/14	320D	5B017
1/00		1/00	350B	5B054
1/24		9/06	660L	5B076

審査請求　未請求　請求項の数12　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－388639(P2001－388639)

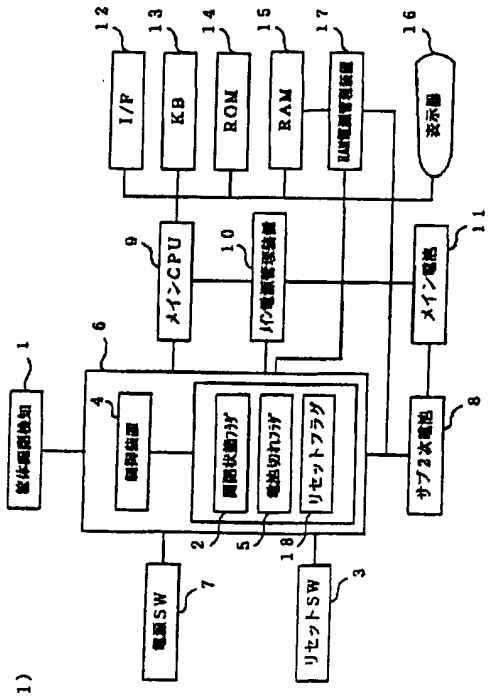
(22)出願日　平成13年12月21日(2001.12.21)

(71)出願人　000104652
キヤノン電子株式会社
埼玉県秩父市大字下影森1248番地
(72)発明者　甘利　隆
埼玉県秩父市大字下影森1248番地　キヤノン電子株式会社内
(74)代理人　100075292
弁理士　加藤　卓

Ｆターム(参考)　5B017 AA03 BA08 BB03 BB05 CA11
CA14
5B054 AA01 AA06 BB08
5B076 FC01 FD04

(54)【発明の名称】　電子機器、電子機器の制御方法、および電子機器の制御プログラム

(57)【要約】
【課題】　電子機器の耐タンパー性とメンテナンス性を両立できるようにする。
【解決手段】　筐体開閉状態フラグ２が過去の筐体の開放を示している時は、リセットスイッチ３によりリセット起動が指令された場合のみ所定のシェルを介した装置の操作を許容し、リセットスイッチ３によりリセット起動が指令されていなければ装置の通常起動を禁止する。シェルを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、筐体開閉状態フラグ２を筐体の閉成を示す状態にリセットする。データ保護は、筐体開閉状態フラグ２が過去の筐体の開放を示している時は、記憶装置（ＲＡＭ１５）の内容を破壊するか、その複写を禁止することにより行なう。



(図1)

1

【特許請求の範囲】

【請求項１】　筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器において、

リセット起動を指令するリセット操作手段と、

前記筐体開閉状態フラグが過去の筐体の開放を示している時は、前記リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止する制御手段を有することを特徴とする電子機器。

【請求項２】　前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットすることを特徴とする請求項１に記載の電子機器。

【請求項３】　前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊することを特徴とする請求項１に記載の電子機器。

【請求項４】　前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止することを特徴とする請求項１に記載の電子機器。

【請求項５】　筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器の制御方法において、

前記筐体開閉状態フラグが過去の筐体の開放を示している時は、前記リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止することを特徴とする電子機器の制御方法。

【請求項６】　前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットすることを特徴とする請求項５に記載の電子機器の制御方法。

【請求項７】　前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊することを特徴とする請求項５に記載の電子機器の制御方法。

【請求項８】　前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止することを特徴とする請求項５に記載の電子機器の制御方法。

【請求項９】　筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器の制御プログラムにおいて、

2

前記筐体開閉状態フラグが過去の筐体の開放を示している時は、前記リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止する制御ステップを含むことを特徴とする電子機器の制御プログラム。

【請求項１０】　前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットする制御ステップを含むことを特徴とする請求項９に記載の電子機器の制御プログラム。

【請求項１１】　前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊する制御ステップを含むことを特徴とする請求項９に記載の電子機器の制御プログラム。

【請求項１２】　前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止する制御ステップを含むことを特徴とする請求項９に記載の電子機器の制御プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器、その制御方法、およびその制御プログラムに関するものである。

【０００２】

【従来の技術】近年、電子商取引が普及するに伴い、電子機器のセキュリティが重要視されるようになってきた。

【０００３】特に、ＰＤＡや携帯電話機、ＩＣカードなどの携帯可能な電子機器に認証情報や個人情報を格納し、これらの情報を用いて決済を行なう電子決済システムが考案されているが、このような電子決済システムの場合、電子機器自体を盗んで内蔵データを読み出すことにより、パスワード、個人情報、顧客情報や金銭情報などの機密性を要する内部データが流出してしまう危険性が考えられる。

【０００４】このため、万が一電子機器が盗まれて第３者の手に渡っても操作できないように、電子機器の起動時にパスワードを要求したり、特別なキーオペレーションを設けたりすることで、内部の情報をプロテクトすることが考えられてきた。

【０００５】しかし、パスワードや特別なキーオペレー

ションによるプロテクトは、機器自体が盗まれたような場合には、記憶装置を取り出して直接アクセスするような行為に対しては充分ではなく、また、機器が小型軽量であればある程、機器の紛失や盗難の可能性は高くなる。

【０００６】また、不正に内部を改造またはリバースエンジニアリングすることにより、ソフトウェアやハードウェアに関する企業秘密やノウハウが流出する問題もある。

【０００７】そこで、電子機器を盗んだ者が筐体を開けて、機密性を要する内部データを読み出したり、不正に内部を改造またはリバースエンジニアリングすることを防ぐために、耐タンパー（Ｔａｍｐｅｒ－Ｐｒｏｏｆ：いたずら防止あるいは不正防止）機能を備えた電子機器も考案されている。たとえば、一度でも機器の筐体が開放された場合、二度と動作しないように制御することにより、耐タンパー機能を実現することができる。

【０００８】

【発明が解決しようとする課題】しかし、前述のように筐体が開放された場合二度と動作しないようにする従来の耐タンパー機能は、第三者の不正な改造やアクセスを防ぐという意味では効果があるが、不便である場合がある。たとえば、実際の運用時における正規のメンテナンス作業での筐体の開閉によっても同様に、以降の動作が出来なくなってしまうという不都合がある。

【０００９】本発明の課題は、上記の問題を解決し、電子機器の耐タンパー性とメンテナンス性を両立できるようにすることにある。

【００１０】

【課題を解決するための手段】上記の課題を解決するため、本発明によれば、筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器、その制御方法、およびその制御プログラムにおいて、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止する構成を採用した。

【００１１】あるいはさらに、前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットする構成を採用した。

【００１２】あるいはさらに、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊する構成を採用した。

【００１３】あるいはさらに、前記筐体開閉状態フラグ

が過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止する構成を採用した。

【００１４】

【発明の実施の形態】以下、図を参照して本発明の実施の形態を説明する。

【００１５】［実施形態１］図１は、本発明を採用した携帯型電子機器の制御系の構造を、図２は、本発明を採用した携帯型電子機器の外観を示している。

【００１６】本実施形態の携帯型電子機器の筐体は、図２に示すように上ケース２１と下ケース２０から構成されており、本携帯型電子機器を分解するためには、不図示の締結ネジを緩めて上ケース２１と下ケース２０を外す必要がある。後述の筐体開閉検知スイッチ１は、上ケース２１と下ケース２０の間の適当な位置に配置されており、上ケース２１と下ケース２０が閉じている状態ではＣｌｏｓｅ信号を、上ケース２１と下ケース２０が空いている状態ではＯｐｅｎ信号を出力するように出来ている。図２中の符号を付した他の部材については、以下、図１に関する説明を参照されたい。

【００１７】図１の制御回路において、筐体開閉検知スイッチ１は、上記の筐体が開けられたことを検出するスイッチであり、本携帯型電子機器の筐体を固定している締結ネジを緩めて、裏蓋を外した時にＯｐｅｎ信号を出力する。このＯｐｅｎ信号は、制御装置４へ割り込み信号として伝達される。

【００１８】開閉状態フラグ２は、後述のサブＣＰＵ６に内蔵されているＲＡＭ１５（後述のように、ＲＡＭ１５の内容は主電源遮断期間においてもバックアップ保持される）上に配置され、過去の筐体開閉検知スイッチ１の状態を記憶する。

【００１９】リセットスイッチ３は、本発明の第１の実施形態である携帯型電子機器のハードウェアリセットを掛けるためのスイッチである。リセットスイッチ３を押すと、まず後述のサブＣＰＵ６に対してリセット信号が出力され、サブＣＰＵ６は割り込み処理により所定のリセットベクタから処理を開始する。

【００２０】リセットフラグ１８は、リセットスイッチ３が押され、サブＣＰＵ６がリセットスタートをした際にセットされるもので、サブＣＰＵ６は後述の電源スイッチ７からの信号によって後述のメインＣＰＵ９へ電源供給を開始する際に、このリセットフラグ１８の状態を信号線を使ってメインＣＰＵ９へ伝える仕様になっている。なお、この情報はメインＣＰＵ９への電源供給を終了する際にクリアするようになっている。

【００２１】制御装置４は、後述のサブＣＰＵ６の中心的存在であり、筐体の開閉状態や後述の電池切れフラグ５の値を元に、メインＣＰＵ９の電源管理を行なうための総合的判断を行なう機能を持つ。

【００２２】電池切れフラグ５は、後述のサブＣＰＵ６に内蔵されたＲＡＭの中に設けられている。具体的に

5

は、このフラグには特定パターンが書き込まれており、通常は後述のサブ２次電池８により内容がバックアップされているが、サブＣＰＵ６に電池切れが起きた時は保持されなくなるため内容が変わる。この変化を制御装置４で判断することにより、電池切れが発生したかを調べるフラグとして扱っている。

【００２３】サブＣＰＵ６は開閉状態フラグ２、電池切れフラグ５、リセットフラグ１８、制御装置４、不図示のＲＯＭやＲＡＭやＩ／Ｆを内蔵している。開閉状態フラグ２、電池切れフラグ５、リセットフラグ１８の状態は、信号線によってメインＣＰＵ９で取得することが可能であるが、それ以外のＲＡＭおよびＲＯＭの内容はサブＣＰＵ６がパッケージ化されているため、外部から調べることは不可能である。なお、サブＣＰＵ６自体は、後述の電源スイッチ７の状態に関わらず、サブ２次電池８によって常に動作を続ける仕様となっている。

【００２４】電源スイッチ７は、本携帯型電子機器の電源投入用スイッチであり、その指示信号はサブＣＰＵ６の制御装置４に入力され、サブＣＰＵ６内で電源供給の許可があった時に、後述のメイン電源管理装置１０へ通電の指示が出る構成になっている。

【００２５】サブ２次電池８は、サブＣＰＵ６の動作及び内蔵ＲＡＭのバックアップ、更にＲＡＭ１５のバックアップに必要な電源を供給するためのものであり、後述のメイン電池１１が外されても電源供給する機能がある。これにより、たとえば筐体を分解しようとしてメイン電池１１を外しても、サブＣＰＵ６だけは動作を続けることが可能となり、筐体が開けられたかどうかを筐体開閉検知スイッチ１の過去の状態を記憶する開閉状態フラグ２により知ることができる。

【００２６】メインＣＰＵ９は、後述のＲＯＭ１４の中のプログラムやデータ、及びＲＡＭ１５の中の変数領域を使って、本携帯型電子機器の動作を制御する。

【００２７】メイン電源管理装置１０は、サブＣＰＵ６からの指示によりメイン電池１１の電力をメインＣＰＵ９及び、インターフェース（Ｉ／Ｆ）１２、キーボード１３、ＲＯＭ１４、ＲＡＭ１５、表示器１６などに供給する。

【００２８】メイン電池１１は、上記メイン電源管理装置１０を経由してメインＣＰＵ９へ電源を供給する他に、メイン電池１１が電子機器に装着されている間、サブ２次電池８へ充電を行なう。

【００２９】インターフェース１２は、本発明の携帯型電子機器が外部デバイス（携帯電話、メモリカード、プリンタなど）と接続する時に使用される。インターフェースの回路構成、通信方式は任意である。

【００３０】キーボード１３は、テンキーや入力キーなどから構成され、データ入力の際に用いられる。表示器１６は、メインＣＰＵ９によって出力結果が描画されることによってメッセージや画像を表示する。

6

【００３１】ＲＯＭ１４は、メインＣＰＵ９が処理を実行する際のプログラムやデータを格納し、ＲＡＭ１５は、メインＣＰＵ９が処理を実行する際、プログラム及び作業用の変数領域に用いられる。

【００３２】ＲＡＭ電源管理装置１７は、サブ２次電池８からの電力をＲＡＭ１５へ送るための機能があり、通常はＲＡＭ１５へ通電し続けてバックアップする仕様になっている。サブＣＰＵ６からの指示によりこの電力供給はカットすることが出来、この場合、バックアップした内容を破壊することが出来る。

【００３３】次に上記構成における動作について説明する。

【００３４】図３は、本実施形態の携帯型電子機器の電源投入時のメインＣＰＵ９が実行するアルゴリズムを示している。

【００３５】電源スイッチ７の押下によりサブＣＰＵ６に電源オンの指示が入ると、サブＣＰＵ６はメイン電源管理装置１０へ電源供給の指示を出すことにより、メインＣＰＵ９が図３のステップＳ０１から動作を開始する。

【００３６】ステップＳ０２では、サブＣＰＵ６内に設けられた電池切れフラグ５の内容を調べ、電池切れが起きている場合はステップＳ０５へ分岐し、電池切れが起きていない場合はステップＳ０３へ進む。

【００３７】ステップＳ０３では、サブＣＰＵ６内に設けられた筐体開閉状態フラグ２の内容を調べ、過去に筐体が開けられた形跡のある場合はステップＳ０６へ、開けられたことのない場合はステップＳ０４へ進む。

【００３８】なお、本電子機器の電池がなくなった場合、サブＣＰＵ６内のＲＡＭの内容は不定になるため、本筐体開閉状態フラグ２の正当性はなくなるが、このような場合は先のステップＳ０２で無条件にデータ破壊の処理に進むので、内部データを不正に吸い上げることは不可能である。

【００３９】ステップＳ０４では、ステップＳ０３で筐体が開けられたことがないと判断されて分岐して来た場合なので、本携帯型電子機器の正常通りの起動処理を行った後、不図示の本来の処理（アプリケーションプログラムの自動実行やシェルの起動）の処理へ制御を移す。

【００４０】ステップＳ０５では、セットされていた電池切れフラグ５をクリアする。これは、メインＣＰＵ９とサブＣＰＵ６を繋ぐ信号線を用いてメインＣＰＵ９からサブＣＰＵ６へ、電池切れフラグ２をクリアするコマンドを発行することにより行なう。

【００４１】ステップＳ０６は、本携帯型電子機器のＲＡＭ１５の内容を破壊する処理である。これはたとえばメモリ内データを全て００でクリアする、または、ＲＡＭ電源管理装置１７からＲＡＭ１５へ供給されるバックアップ電源を切ることにより行なう。

【００４２】次に、ステップＳ０７でリセットフラグ１

7

８を参照し、今回の起動がリセットスイッチ２を押下してから１回目の起動か否かを調べる。起動の直前にリセットスイッチ１８が押下されていなかった場合、ステップＳ０９でメインＣＰＵ９から信号線を使ってサブＣＰＵ６に電源オフ要求を出すことで、メイン電源管理装置１０からの電源供給を切って装置全体の電源を遮断する。

【００４３】ステップＳ０７でリセット直後の起動であることが分かった場合、ステップＳ０８でシェルを起動する。

【００４４】図４は、ステップＳ０８で起動されるシェルのアルゴリズムを示したフローチャートである。シェルとはオペレータがキーボード１３から入力した文字列をコマンドとして解釈して、そのコマンドを実行するプログラムであり、たとえば、ＵＮＩＸ（商標名）においてはｓｈ、ｃｓｈなど、ＭＳ－ＤＯＳにおいてはＣＯＭＭＡＮＤ．ＣＯＭなどが代表的である。本実施形態においては、これら一般のシェルに機能を一部追加しており、以下のようなアルゴリズムになっている。

【００４５】まず、ステップＳ１２で、本携帯型電子機器のキーボード１３からコマンド文字列が入力される。

【００４６】次にステップＳ１３で、この文字列が記憶装置のフォーマット（初期化）を命令するコマンド名に一致する場合はステップＳ１４へ分岐、それ以外の時はステップＳ１５へ分岐する。記憶装置のフォーマットを行なうコマンド名は任意でよく、また必要な場合にはコマンド名に続きコマンドライン引数が後置される仕様でもよい。好ましくはこのコマンドの実体は別ファイルではなく、シェルの内部コマンドとして実装するのがよい。

【００４７】ステップＳ１３で、入力された文字列が記憶装置の初期化コマンドであった場合、ステップＳ１４でサブＣＰＵ６内のリセットフラグ１８の内容をクリアする。このクリア処理は、たとえばメインＣＰＵ９とサブＣＰＵ６を繋ぐ信号線を用いてメインＣＰＵ９からサブＣＰＵ６へ、開閉状態フラグ２をクリアするコマンドを発行することにより行なう。

【００４８】ステップＳ１５は、一般のシェルが備えている機能をそのまま実行する処理である。ここではファイルのコピーや外部コマンドの実行などを行なうが、もちろん、初期化コマンドがステップＳ１２で入力された場合には、ステップＳ１４で開閉状態フラグ２をクリアした後、指定された初期化処理を行なう。なお、ステップＳ１５は単一のステップとして記載してあるが、ここでは、コマンド入力～実行のイベントループを実行してもよいし、また、単に１つのコマンド入力とその実行を行なうだけでもよい。

【００４９】図５は、本携帯型電子機器のサブＣＰＵ６のアルゴリズムを示している。

【００５０】サブＣＰＵ６には電源スイッチはなく、メイン電池１１が装着されると直ちに動作を開始し、以後常に動作を続ける仕様になっている。そのため、図５に示したフローチャートでは処理の終了を意味するブロックがないが、これで問題はない。

8

【００５１】また、メイン電池１１から供給される電力はサブ２次電池８に充電されているため、メイン電池１１を外していてもサブ２次電池８からの電力によって、サブＣＰＵ６は動作を続けることが出来る。

【００５２】サブＣＰＵ６をステップＳ２１から処理を実行させるには、前述の通りメイン電池１１を装着する以外に、リセットスイッチ３を押下しリセットベクタから再起動することでも可能である。

【００５３】ステップＳ２２で、サブＣＰＵ６内のリセットフラグ１８をセットし、リセット起動した旨を記憶する。この情報は、後にメインＣＰＵ９から情報取得コマンドが送られてきた際にメインＣＰＵ９へ通知される。

【００５４】不図示の初期設定処理などを行った後、サブＣＰＵ６はステップＳ２３でＨＡＬＴモードへ移行する。このＨＡＬＴモードはサブＣＰＵ６の消費電力を低くするモードとしてＣＰＵチップに実施されている公知のものでよい。通常、ＨＡＬＴモードでは、動作に必要なクロック信号の停止、外部バスへのアクセス禁止などが行なわれる。ＨＡＬＴモードではサブＣＰＵ６は、電源スイッチ７からの押下信号を割り込み入力で待機している。

【００５５】電源スイッチ７からの割り込み信号が通知されると、ステップＳ２４でメイン電源管理装置１０へ電源供給開始の指示を出し、メインＣＰＵ９の動作を開始させる。以降は、メインＣＰＵ９から信号線を経由して送られてくる各種コマンドに対して応答するという処理を実行する。リセットフラグ１８の内容を取得するコマンドも、ここで入力、処理される。

【００５６】ステップＳ２５で、メインＣＰＵ９から入力されるコマンドを取り込み、ステップＳ２６で、この内容を解析する。解析の結果、電源オフ要求コマンドではなかった場合は、その内容に応じた処理をステップＳ２９で実行した後、再度ステップＳ２５へ進み、コマンド入力待ちになる。メインＣＰＵ９から入力されたコマンドが電源オフ要求コマンドの場合はステップＳ２７へ分岐する。

【００５７】ステップＳ２７は、前述のステップＳ２４と同様に、メイン電源管理装置１０へ電源供給終了の指示を出しメインＣＰＵ９の動作を終了させる。

【００５８】ステップＳ２８は、サブＣＰＵ６内のリセットフラグ１８をクリアし、以降はリセット起動していない旨を記憶する。その後、サブＣＰＵ６の処理は再びステップＳ２３の低消費電力モードに移行する。

【００５９】次に、以上のような本実施形態の携帯型電子機器の運用について具体的に説明する。

9

【００６０】まず、本携帯型電子機器が工場で組み立てられて一番初めに電源が投入された時は、図３のフローチャートにおいては、ステップＳ０１→ステップＳ０２→ステップＳ０５→ステップＳ０６→ステップＳ０７→ステップＳ０９→ステップＳ１０となり、すぐに電源がオフされる。

【００６１】そこで次に、リセットスイッチ３を押下してから電源を投入すると、ステップＳ０１→ステップＳ０２→ステップＳ０３→ステップＳ０６→ステップＳ０７→ステップＳ０８となり、シェルが起動する。ここで、初期化処理を行なうと、ステップＳ１４で筐体開閉状態フラグ２がクリアされ、ステップＳ１０で終了する。

【００６２】次に電源をオンすると、ステップＳ０１→ステップＳ０２→ステップＳ０３→ステップＳ０４→ステップＳ１０となり、以降は全く普通の操作が行え、ユーザにはこの状態で出荷される。

【００６３】ユーザは、出荷された本携帯型電子機器に対して必要であればアプリケーションプログラムを追加し、さらに自己の運用に必要なデータ（パスワードや個人情報など機密性の高いものも含まれる）をＲＡＭ１５にインストールし、業務に利用する。

【００６４】ここで筐体を開けるとサブＣＰＵ６内の筐体開閉状態フラグ２がセットされ、次に電源を投入した時、ステップＳ０１→ステップＳ０２→ステップＳ０３→ステップＳ０６→ステップＳ０７→ステップＳ０９→ステップＳ１０となりすぐに電源が切れてしまう。つまり悪意を持ったものが携帯型電子機器を分解して内部に細工を施しても、次からは２度と起動しなくなる。

【００６５】ただし、この筐体を開けるという行為は正規のメンテナンス時にも必須の作業であり、このまま２度と使えなくなってしまうというのは非常に使い勝手が悪い。

【００６６】しかし、本実施形態によれば、リセットスイッチ３を押下した後、電源を投入するとステップＳ０１→ステップＳ０２→ステップＳ０３→ステップＳ０６→ステップＳ０７→ステップＳ０８となり、シェルが起動する。この時点で、シェルからＲＡＭ１５の内容を初期化するコマンドを実行すると、筐体開閉状態フラグ２がクリアされ、以降は再び通常起動および運用が可能になる。

【００６７】以上のように、本実施形態によれば、機器の筐体を開放した場合は、機器の内部データを破壊し、筐体開閉状態フラグをセットすることにより、以後、通常の起動方法では２度と装置を起動できないように制御する。これにより、機器の記憶装置に格納されたパスワードや個人情報などを確実に保護できる。本実施形態によれば、内蔵されていたアプリケーションのリバースエンジニアリングや機密情報を盗み出すことは不可能となる。

10

【００６８】また、機器の筐体を開放したとしても、リセット操作を行なった後、電源を投入すれば、シェルを起動することができ、ここで記憶装置の初期化操作を行なえば、記憶装置の初期化を実行するとともに筐体開閉状態フラグをリセットできるので、通常の起動操作を再び有効とし、容易に機器を再運用可能な状態に戻すことができる。

【００６９】本実施形態においては、機器の筐体を開放した場合は、機器の内部データを無条件で破壊し、かつ、通常の起動操作を可能とするためには記憶装置の初期化を実行しなければならないので、たとえサービスマンが悪意をもって顧客のデータを盗もうとしてもそのような不正な内部データアクセスは一切行なえない。

【００７０】なお、図４の制御において、ステップＳ１３で初期化コマンドが指令されなかった場合はステップＳ１５に移行するようにしているが、ステップＳ１３で初期化コマンドが指令されなかった場合は処理を中止し、電源を遮断するようにしてもよい。つまり、初期化コマンドを実行した場合のみ、開閉状態フラグ２のクリアとコマンド実行（ないしコマンド実行ループ）を許容するようにする。あるいは、ステップＳ１３で初期化コマンドが指令されなかった場合は、ステップＳ１５に移行できるが、ステップＳ１５で実行できるコマンドに制限を加えるようにしてもよい。

【００７１】［実施形態２］先の実施形態では筐体が開けられた場合、ステップＳ０６においてメモリ内データを全て００でクリアする、または、ＲＡＭ電源管理装置１７からＲＡＭ１５へ供給されるバックアップ電源を切ることでＲＡＭ１５の内容を破壊していた。これは、ステップＳ０８でシェルを起動した際に、複写コマンド（たとえば、ＭＳ－ＤＯＳではＣＯＰＹコマンド）を使って、ＲＡＭ１５内のファイルをインターフェース１２を介して外部記憶装置に複写されてしまうことを防ぐためである。

【００７２】ところが、実際にはメモリ内データを全て００でクリアするのには若干の時間が必要になる。特に近年の大容量のメモリを積んだ携帯型電子機器においてはかなりの時間を要する場合もある。また、ＲＡＭ１５への電源供給を管理するＲＡＭ電源管理装置１７を設けることは電子機器の製造コストアップに繋がるため、好ましくない。

【００７３】そこで、本発明第２の実施形態では上記問題を鑑みて、以下の処理を行なう。

【００７４】まず、図３の中からステップＳ０６（データ破壊処理）を除去したものが、第２の実施形態のメインＣＰＵ９のアルゴリズムとなる。本実施形態のメインＣＰＵ９のアルゴリズムは、それ以外では図３と全く同様であるものとする。

【００７５】図６は本実施形態のシェルのアルゴリズムを示している。ステップＳ３１からステップＳ３６まで

は、それぞれ前述の図４のステップＳ１１からステップＳ１６と同じ機能であるため、説明は省略する。

【００７６】図６では、ステップＳ３３で入力されたコマンドが初期化コマンドではなかった場合はステップＳ３７に分岐する。ここでは、更に入力されたコマンドが複写コマンド（たとえば、ＭＳ－ＤＯＳではＣＯＰＹコマンド）かどうかを調べ、複写コマンドではなかった場合ステップＳ３８へ分岐する。しかし、複写コマンドの場合は何もせずステップＳ３６へ分岐してそのまま終了する。

【００７７】ステップＳ３８では、入力されたコマンドが（シェルの内臓コマンドではない）外部コマンドかどうか調べ、外部コマンドではなかった場合、ステップＳ３５へ分岐し、そのままコマンドを実行する。しかし、外部コマンドの場合は何もせず、ステップＳ３６へ分岐してそのまま終了する。

【００７８】このようにして、図６で示すようにシェルを実装しておくことにより、図３のステップＳ０６がなくても、電子機器の内部データを複写することができなくなるので、これにより電子機器の内部データを保護することができる。本実施形態では、データ破壊を行なわないので、ＲＡＭ電源管理装置１７、あるいは少なくともものそのデータ破壊機能は不要であり、製造コストを低減し、また、筐体開放時のタンパープルーフ動作は筐体開放フラグのセットだけで済むのでより迅速に実行できる。

【００７９】本実施形態２の構成によれば、電子機器の内部データを消去せず、その複写を行なえなくするようにしている他に、専用のプログラムを用意しても内部データをバックアップコピーすることはできない。

【００８０】なお、筐体を開放した後は通常の起動が不可能となり、リセット操作によりシェルを起動し、そこで初期化コマンドを入力することにより再運用可能な状態に復帰させる動作については、上記実施形態１と同様である。

【００８１】以上では、ディスプレイとキーボードを有する小型の携帯型電子機器を例示したが同様の技術は携帯電話機やＰＤＡ、ＩＣカードなど内部に保護すべきデータ（パスワード、個人情報、あるいは企業秘密を含むアプリケーションプログラム、プログラムデータなど）を記憶する電子機器に広く実施することができる。また、以上ではシェルとしてｓｈ、ｃｓｈ、ｃｏｍｍａｎｄ．ｃｏｍなど、コマンドラインインターフェースを用いるものを例示したが、シェルのユーザーインターフェース方式は任意であり、ＧＵＩを用いたものであってもよい。また、本発明に関しては、シェルは少なくともリセット後のメンテナンス作業で利用できればよく、通常の起動後、ユーザがこのシェルを用いて装置の操作を行なう構成でなくてもよいのはいうまでもない。

【００８２】本発明の制御プログラムは、ＲＯＭ１４などに格納して装置とともに供給することができる他、ネットワークやインターフェース１２を介してダウンロードすることによりインストールやアップグレードが行なえるような構成であってもよい。また、以上ではＣＰＵがメイン／サブの２つに分かれた構成を例示したが、このような複数ＣＰＵの構成は必ずしも必須のものではない。

【００８３】

【発明の効果】以上の説明から明らかなように、本発明によれば、筐体の開放を検出する筐体開放検知手段と、前記筐体開放検知手段の検出状態を記憶する筐体開閉状態フラグを有し、いったん筐体が開放されると、以後、装置の通常起動を禁止する電子機器、その制御方法、およびその制御プログラムにおいて、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、リセット操作手段によりリセット起動が指令された場合のみ所定のユーザーインターフェースを介した装置の操作を許容し、前記リセット操作手段によりリセット起動が指令されていなければ装置の通常起動を禁止する構成を採用しているので、いったん筐体が開放されると、以後、装置の通常起動を禁止することにより、内部データの取り出し、リバースエンジニアリングなどの不正な装置の使用を防止できるとともに、リセット操作手段によりリセット操作を行なえば所定のユーザーインターフェースを介した装置の操作が可能となるため、装置のメンテナンスを行なうことができ、電子機器の耐タンパー性とメンテナンス性を両立できる、という優れた効果がある。

【００８４】あるいはさらに、前記所定のユーザーインターフェースを介した装置の操作においては、内部のデータ記憶装置を初期化することによって、前記筐体開閉状態フラグを筐体の閉成を示す状態にリセットする構成を採用することにより、内部のデータ記憶装置の初期化を条件として装置の通常起動を行なえるよう復帰させることができる。

【００８５】あるいはさらに、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容を破壊する構成、あるいは、前記筐体開閉状態フラグが過去の筐体の開放を示している時は、内部のデータ記憶装置の内容の複写を禁止する構成によれば、確実にデータ記憶装置のデータ内容を保護することができる、という優れた効果がある。特に、内部のデータ記憶装置の内容を破壊せず、複写の禁止のみを行なう構成においては、ユーザデータを損なうことなく装置の修理／保守作業を行なえる、という利点がある。

【図面の簡単な説明】

【図１】本発明を採用した携帯型電子機器のブロック図である。

【図２】図１の携帯型電子機器の外観図である。

【図３】本発明の第１実施形態の電源投入時の制御を示したフローチャート図である。

13

【図４】本発明の第１実施形態のシェルの制御を示したフローチャート図である。

【図５】本発明の第１実施形態のサブＣＰＵの制御を示したフローチャート図である。

【図６】本発明の第２実施形態のシェルの制御を示したフローチャート図である。

【符号の説明】

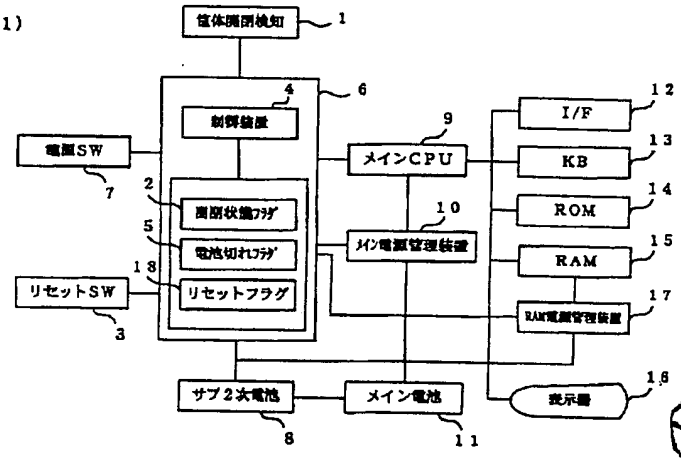
1　筐体開閉検知スイッチ
2　筐体開閉状態フラグ
3　リセットスイッチ
4　制御装置
5　電池切れフラグ
6　サブＣＰＵ
7　電源スイッチ

14

8　サブ２次電池
9　メインＣＰＵ
１０　メイン電源管理装置
１１　メイン電池
１２　インターフェース
１３　キーボード
１４　ＲＯＭ
１５　ＲＡＭ
１６　表示器
１７　ＲＡＭ電源管理装置
１８　リセットフラグ
２０　下ケース
２１　上ケース

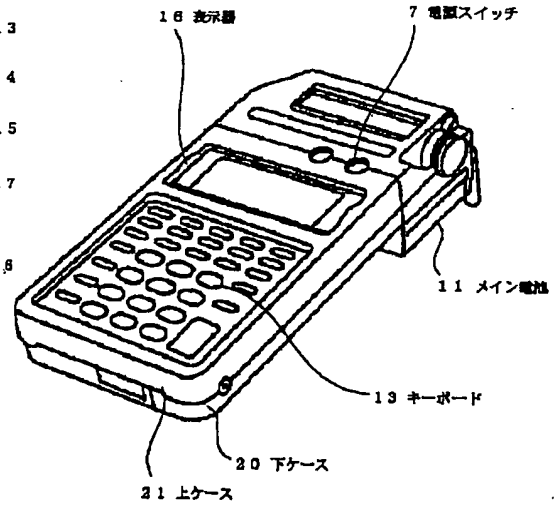
【図１】

(図1)



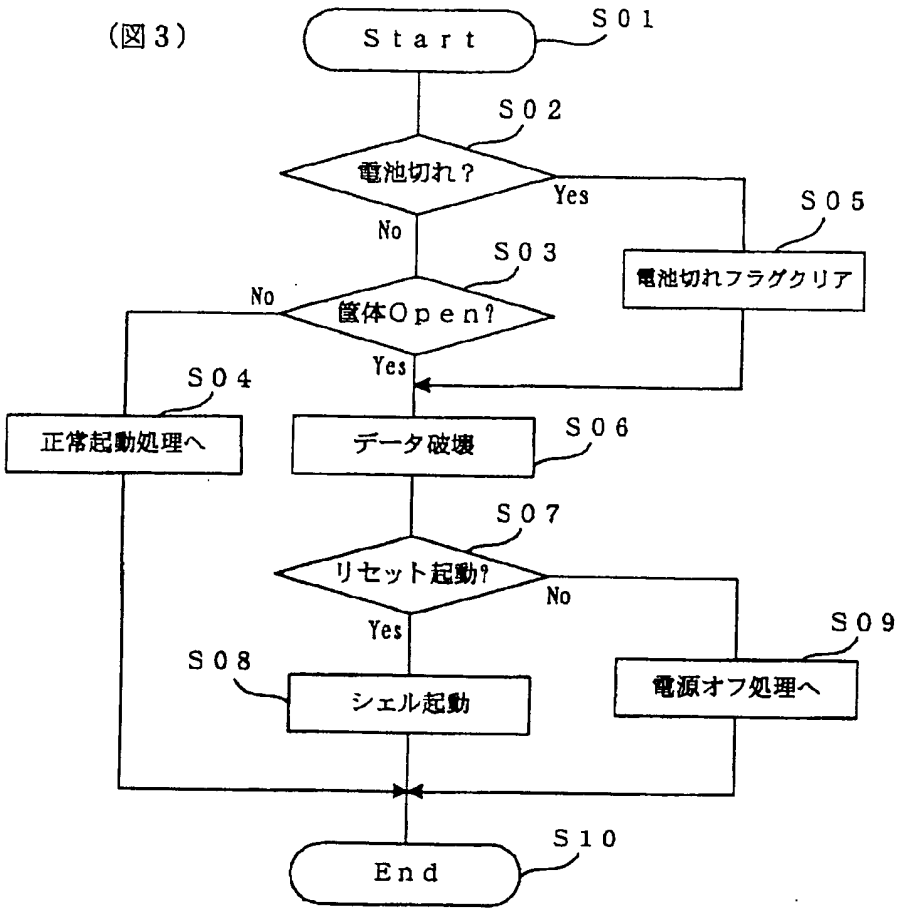
【図２】

(図2)



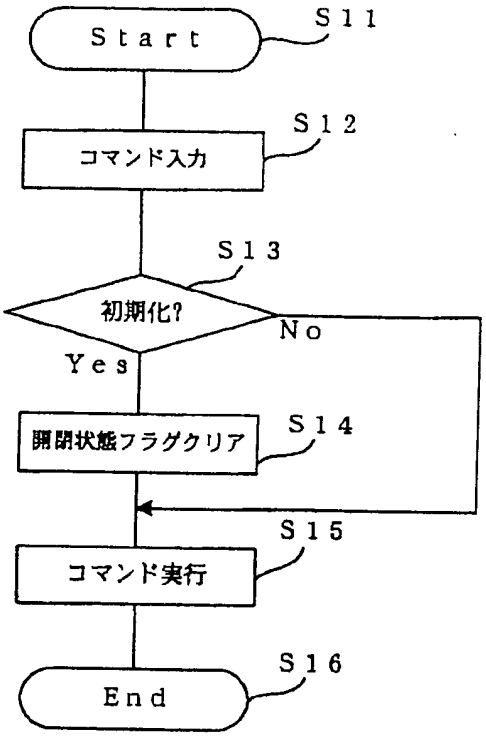
【図３】

(図３)

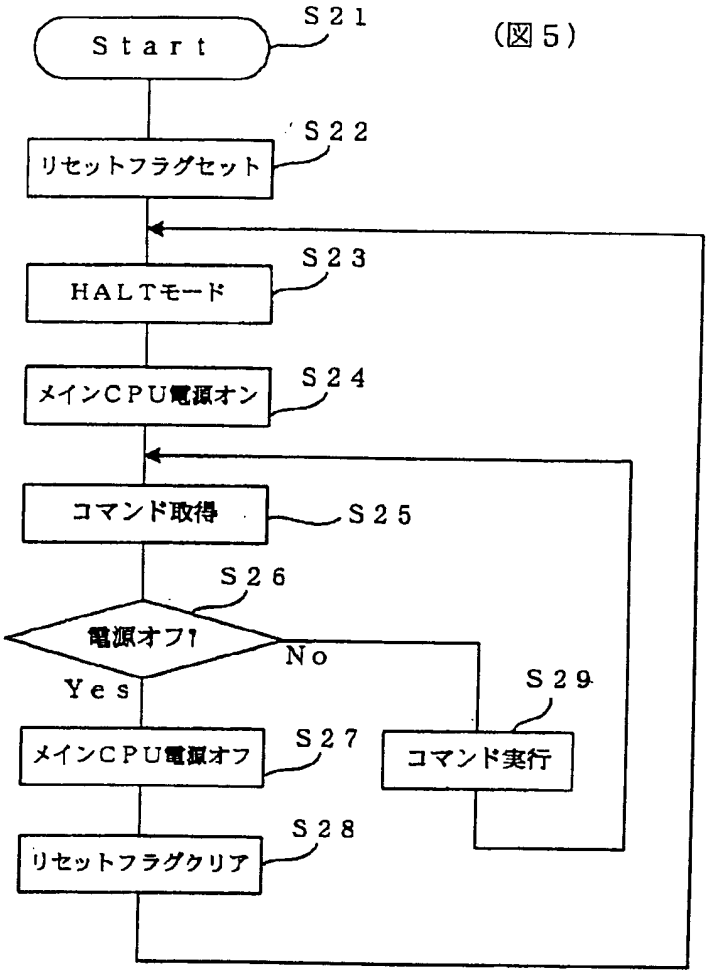

Ｓｔａｒｔ
Ｓ０１
Ｓ０２
電池切れ？
Yes
No
Ｓ０５
電池切れフラグクリア
Ｓ０３
No
筐体Ｏｐｅｎ?
Yes
Ｓ０４
正常起動処理へ
データ破壊
Ｓ０６
Ｓ０７
リセット起動?
No
Yes
Ｓ０９
Ｓ０８
シェル起動
電源オフ処理へ
Ｓ１０
Ｅｎｄ

【図４】

(図４)


Start
S11
コマンド入力
S12
初期化?
S13
No
Yes
開閉状態フラグクリア
S14
コマンド実行
S15
End
S16

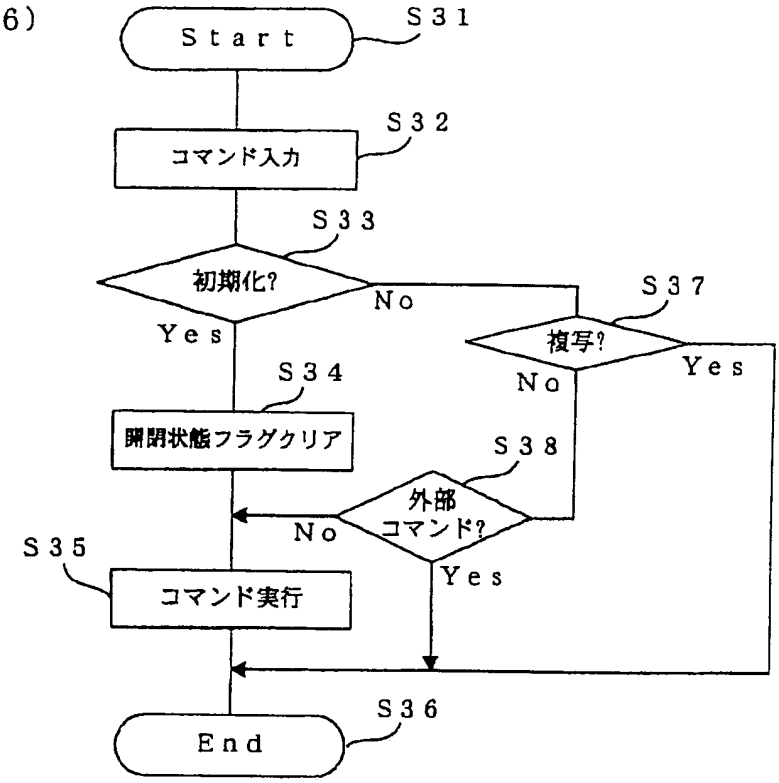
【図５】


Ｓｔａｒｔ
Ｓ２１
リセットフラグセット
Ｓ２２
ＨＡＬＴモード
Ｓ２３
メインＣＰＵ電源オン
Ｓ２４
コマンド取得
Ｓ２５
Ｓ２６
電源オフ？
Ｎｏ
Ｙｅｓ
Ｓ２９
メインＣＰＵ電源オフ
Ｓ２７
コマンド実行
リセットフラグクリア
Ｓ２８

(図５)

【図６】

(図６)


Start
S31
コマンド入力
S32
S33
初期化?
No
Yes
S37
複写?
No
Yes
S34
開閉状態フラグクリア
S38
外部
コマンド?
No
Yes
S35
コマンド実行
End
S36